# Magerit vs. ISO 27005

11.6.2015

## 1 Map Magerit to 27005

| **magerit v3** | **27005:2011** |
|---|---|
| step 1 – assets | 8.2.2 Identification of assets<br>B.1 Examples of asset identification |
| • dependencies | B.2 Asset valuation |
| • valuation | B.2 Asset valuation |
| step 2 – threats | |
| • identification | 8.2.3 Identification of threats |
| • valuation | 8.2.5 Identification of vulnerabilities<br>8.2.6 Identification of consequences<br>8.3.2 Assessment of consequences<br>8.3.3 Assessment of incident likelihood |
| • potential impact | |
| • potential risk | |
| step 3 – safeguards | 8.2.4 Identification of existing controls<br>8.2.5 Identification of vulnerabilities<br>9. Information security risk treatment |
| • selection | See 27001:2013<br>6.1.3 Information security risk treatment |
| step 4 – residual impact | |
| step 5 – residual risk | 8.3.4 Level of risk determination<br>10. Information security risk acceptance |

| **magerit v3** | **27005:2011** |
|---|---|
| RAM.1 – Characterization of assets | |
| RAM.11 – Identification of assets | 8.2.2 Identification of assets<br>B.1 Examples of asset identification |
| RAM.12 – Dependencies between assets | B.2 Asset valuation |
| RAM.13 – Valuation of assets | B.2 Asset valuation |
| RAM.2 – Characterization of threats | |
| RAM.21 – Identification of threats | 8.2.3 Identification of threats |
| RAM.22 – Valuation of threats | 8.2.6 Identification of consequences<br>8.3.2 Assessment of consequences<br>8.3.3 Assessment of incident likelihood |
| RAM.3 – Characterization of safeguards | |
| RAM.31 – Identification of relevant safeguards | See 27001:2013<br>6.1.3 Information security risk treatment |
| RAM.32 – Evaluation of safeguards | 8.2.4 Identification of existing controls |
| RAM.4 – Risk status estimate | |
| RAM.41 – Impact estimate | |
| RAM.42 – Risk estimate | 8.3.4 Level of risk determination |

# 2 Map 27005 to Magerit

| **27005:2011** | **magerit v3** |
|---|---|
| 8.2 Risk identification | |
| 8.2.1 Introduction to risk identification | |
| 8.2.2 Identification of assets | RAM.11 – Identification of assets |
| 8.2.3 Identification of threats | RAM.21 – Identification of threats |
| 8.2.4 Identification of existing controls | RAM.32 – Evaluation of safeguards |
| 8.2.5 Identification of vulnerabilities | RAM.21 – Identification of threats<br>RAM.22 – Valuation of threats<br>RAM.32 – Evaluation of safeguards |
| 8.2.6 Identification of consequences | RAM.22 – Valuation of threats |
| 8.3 Risk analysis | |
| 8.3.1 Risk analysis methodologies | |
| 8.3.2 Assessment of consequences | RAM.22 – Valuation of threats |
| 8.3.3 Assessment of incident likelihood | RAM.22 – Valuation of threats |
| 8.3.4 Level of risk determination | RAM.42 – Risk estimate |
| 8.4 Risk evaluation | |
| 9. Information security risk treatment | Magerit: 4. Risk management process |
| 10 Information security risk acceptance | Magerit: 4.1.2 Risk acceptance |
| 12 Information security risk monitoring and review | |
| 12.1 Monitoring and review risk factors | |
| 12.2 Risk management, monitoring, reviewing and improving | |
| B Identification and valuation of assets and impact assessment | |
| B.1 Examples of asset identification | |
| B.1.1 The identification of primary assets | essential assets |
| B.1.2 List and description of supporting assets | other assets |
| B.2 Asset valuation | dependencies<br>asset valuation |
| B.3 Impact assessment | threat valuation: degradation |